世界知的所有権機関
国際事務局

PCT

特許協力条約に基づいて公開された国際出願

(51) 国際特許分類7
H04L 9/08, 9/32, 12/40, H04N 7/167

A1

(11) 国際公開番号 WO00/62476

(43) 国際公開日 2000年10月19日(19.10.00)

(21) 国際出願番号 PCT/JP00/02354

(22) 国際出願日 2000年4月11日(11.04.00)

(30) 優先権データ
特願平11/105965 1999年4月13日(13.04.99) JP

(71) 出願人（米国を除くすべての指定国について）
ソニー株式会社(SONY CORPORATION)[JP/JP]
〒141-0001 東京都品川区北品川6丁目7番35号 Tokyo, (JP)
(72) 発明者；および
(75) 発明者／出願人（米国についてのみ）
浅野智之(ASANO, Tomoyuki)[JP/JP]
大澤義知(OSAWA, Yoshitomo)[JP/JP]
小室輝芳(KOMURO, Teruyoshi)[JP/JP]
石黒隆二(ISHIGURO, Ryuji)[JP/JP]
〒141-0001 東京都品川区北品川6丁目7番35号
ソニー株式会社内 Tokyo, (JP)
(74) 代理人
小池 晃, 外(KOIKE, Akira et al.)
〒105-0001 東京都港区虎ノ門二丁目6番4号
第11森ビル Tokyo, (JP)

(81) 指定国 JP, US

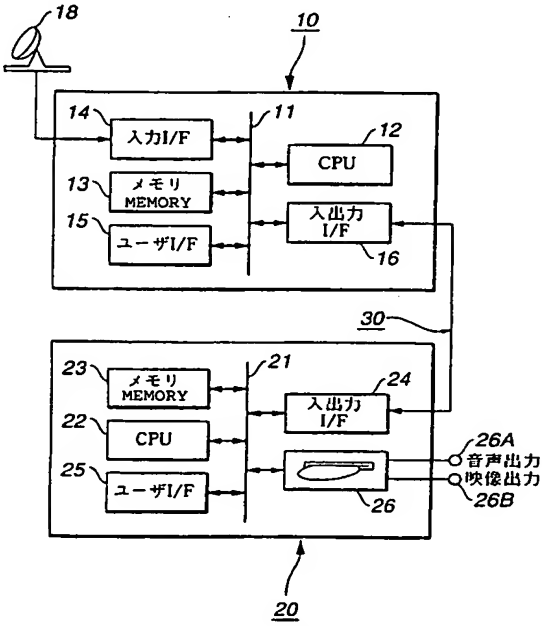
添付公開書類
国際調査報告書

(54)Title: DATA TRANSMISSION SYSTEM

(54)発明の名称 データ伝送システム

(57) Abstract

An encryption key is produced by 1st information owned secretly in common with a data receiver (20), 2nd information introduced from duplication control information of transmission data and 3rd information which is time modulation information owned in common with the data receiver. Data are encrypted by a CPU (12) using the encryption key. Transmission data which are obtained by adding the duplication control information data and the time modulation information to the encrypted data are transmitted to the data receiver (20) from a data transmitter (10).



14...INPUT INTERFACE
24...I/O INTERFACE
15...USER INTERFACE
25...USER INTERFACE
16...I/O INTERFACE
26A...VOICE OUTPUT
26B...IMAGE OUTPUT

BNSDOCID: <WO___0062476A1_I_>

(57)要約

データ受信装置２０との間で秘密に共有されている第１の情報と、送信データの複製制御情報から導かれる第２の情報と、上記データ受信装置との間で共有する時変情報である第３の情報によって暗号鍵を生成し、この暗号鍵を用いてデータをＣＰＵ１２により暗号化し、暗号化したデータに時変情報を上記複製制御情報及び時変情報を付加した送信データをデータ送信装置１０からデータ受信装置２０に送信する。

PCTに基づいて公開される国際出願のパンフレット第一頁に掲載されたPCT加盟国を同定するために使用されるコード(参考情報)

AE アラブ首長国連邦
AG アンティグア・バーブーダ
AL アルバニア
AM アルメニア
AT オーストリア
AU オーストラリア
AZ アゼルバイジャン
BA ボズニア・ヘルツェゴビナ
BB バルバドス
BE ベルギー
BF ブルギナ・ファソ
BG ブルガリア
BJ ベナン
BR ブラジル
BY ベラルーシ
CA カナダ
CF 中央アフリカ
CG コンゴー
CH スイス
CI コートジボアール
CM カメルーン
CN 中国
CR コスタ・リカ
CU キューバ
CY キプロス
CZ チェッコ
DE ドイツ
DK デンマーク
DM ドミニカ
DZ アルジェリア
EE エストニア
ES スペイン
FI フィンランド
FR フランス
GA ガボン
GB 英国
GD グレナダ
GE グルジア
GH ガーナ
GM ガンビア
GN ギニア
GR ギリシャ
GW ギニア・ビサオ
HR クロアチア
HU ハンガリー
ID インドネシア
IE アイルランド
IL イスラエル
IN インド
IS アイスランド
IT イタリア
JP 日本
KE ケニア
KG キルギスタン
KP 北朝鮮
KR 韓国
KZ カザフスタン
LC セントルシア
LI リヒテンシュタイン
LK スリ・ランカ
LR リベリア
LS レソト
LT リトアニア
LU ルクセンブルグ
LV ラトヴィア
MA モロッコ
MC モナコ
MD モルドヴァ
MG マダガスカル
MK マケドニア旧ユーゴスラヴィア共和国
ML マリ
MN モンゴル
MR モーリタニア
MW マラウイ
MX メキシコ
MZ モザンビーク
NE ニジェール
NL オランダ
NO ノールウェー
NZ ニュー・ジーランド
PL ポーランド
PT ポルトガル
RO ルーマニア
RU ロシア
SD スーダン
SE スウェーデン
SG シンガポール
SI スロヴェニア
SK スロヴァキア
SL シエラ・レオネ
SN セネガル
SZ スワジランド
TD チャード
TG トーゴー
TJ タジキスタン
TM トルクメニスタン
TR トルコ
TT トリニダッド・トバゴ
TZ タンザニア
UA ウクライナ
UG ウガンダ
US 米国
UZ ウズベキスタン
VN ヴェトナム
YU ユーゴースラヴィア
ZA 南アフリカ共和国
ZW ジンバブエ

BNSDOCID: <WO 0062476A1 >

明細書

データ伝送システム

技術分野

本発明は、データ送信装置からデータ受信装置にデータを伝送するデータ伝送システム、データ伝送方法、データ送信装置、データ送信方法、データ受信装置及びデータ受信方法に関する。

背景技術

近年、例えば家庭内において、複数のＡＶ機器をデジタルインターフェースを介して接続し、音楽情報や映像情報などのデジタルデータを伝送したり記録したりするようにしたシステムが普及しつつある。例えば、デジタルバスであるＩＥＥＥ(The International of Electrical and Electronics Engineers,Inc.)１３９４ハイ・パフォーマンス・シリアル・バス規格（以下、単にＩＥＥＥ１３９４シリアルバスという）のインターフェースを持つビデオカメラやDigital Versatile Disk(DVD)(商標）プレーヤなどのＡＶ機器が開発されている。

ところで、通常、映画データ等は著作権のある情報であり、不正

BNSDOCID: <WO___0062476A1_I_>

なユーザによるコピー等を防ぐ必要がある。

不正なユーザによるコピー等を防ぐために、例えば、ミニディスク(MD)(商標)システムにおいては、ＳＣＭＳ(Serial Copy Management System)と呼ばれる方法が用いられている。これは、デジタルインタフェースによって、音楽データとともに伝送される情報のことである。この情報は、音楽データが、copy free、copy once allowed、又はcopy prohibited のうちのいずれのデータであるのかを表す。ミニディスクレコーダは、デジタルインタフェースから音楽データを受信した場合、ＳＣＭＳを検出し、これが、copy prohibited であれば、音楽データをミニディスクに記録せず、copy once allowed であれば、SCMS情報をcopy prohibited に変更すると共に、受信した音楽データとともに記録し、copy freeであれば、SCMS情報はそのままで受信した音楽データとともに記録する。

このようにして、ミニディスクシステムにおいては、ＳＣＭＳを用いて、著作権を有するデータが不正にコピーされるのを防いでいる。

また、デジタルインタフェースを介して音楽情報や映像情報などのデジタルデータを伝送したり記録したりするようにしたデータ伝送システムでは、伝送路上のデータパケットのパケットヘッダに、複製制御情報を格納して送る方式が考えられている。

この複製制御情報は、例えば次のように

００：コピー制限なし

１０：１回のみコピー可

０１：これ以上のコピー禁止

１１：もともとコピー禁止２ビットで定義されている。

データパケットを受信した記録機器は、データを記録する際に、複製制御情報を検査し、複製制御情報が「０１」又は「１１」すなわちコピー禁止を表していれば受信したデータの記録を行わない。また、複製制御情報が「１０」すなわち１回のみコピー可を表していれば、複製制御情報を「０１」すなわちこれ以上のコピー禁止に変更してから受信データを記録メディアに記録する。

このようにして、もとのデータから生じるコピーの世代を制限するようにしている。

さらに、このコピー世代の制限方式に強制力を持たせるために、データを暗号化して伝送し、コピー世代制限方式を遵守する機器のみを製造するという契約を交わしたメーカーにのみ、暗号化及び復号に必要な情報をライセンスするなどの方法も用いられている。

ところで、伝送路上のデータパケットのパケットヘッダに複製制御情報を格納して送る方式では、パケットが送信機器から受信機器に伝送される過程で、複製制御情報が他の機器により改竄される可能性がある。

例えば、図１に示すように、データ送信装置１側からデータパケットのパケットヘッダの複製制御情報をコピー禁止の意味を表す「１１」で送信しても、伝送中に複製制御情報改竄攻撃があり、複製制御情報が１回コピー可を表す「１０」に改竄されてしまうと、このパケットを受信したデータ受信装置２側では、このデータが本来コピー禁止であることを知ることができず、パケットヘッダの複製制御情報が１度の記録を許しているのでデータを記録してしまう。

このように、従来のデータ伝送方法では、コピー世代管理ができなくなってしまう恐れがある。

BNSDOCID: <WO__0062476A1 | >

発明の開示

そこで、本発明の目的は、上述の如き従来の問題点に鑑み、コピー世代管理を確実に行うことができるデータ伝送システム、データ伝送方法、データ送信装置、データ送信方法、データ受信装置及びデータ受信方法を提供することにある。

本発明に係るデータ伝送システムは、データ受信装置との間で秘密に共有されている第１の情報と、データの複製制御情報から導かれる第２の情報と、上記データ受信装置との間で共有する時変情報である第３の情報に基づいて暗号鍵を生成し、上記暗号鍵を用いてデータを暗号化し、暗号化したデータに上記複製制御情報及び時変情報に基づく制御情報を付加した送信データを送信するデータ送信装置と、上記データ送信装置から送られてくる制御情報が付加され暗号化されたデータを受信し、上記データ送信装置との間で秘密に共有されている第１の情報と、上記受信データの制御情報から導かれる第２の情報と、上記データ送信装置との間で共有する時変情報である第３の情報に基づいて暗号鍵を生成し、上記暗号鍵を用いて上記受信データを復号するデータ受信装置とからなる。

また、本発明に係るデータ伝送方法では、データ送信装置とデータ受信装置の間で秘密に共有されている第１の情報と、送信データの複製制御情報から導かれる第２の情報と、データ受信装置との間で共有する時変情報である第３の情報によって生成された暗号鍵を用いてデータを暗号化して伝送する。

また、本発明に係るデータ伝送方法では、データ送信装置において、データ受信装置との間で秘密に共有されている第１の情報と、データの複製制御情報から導かれる第２の情報と、上記データ受信装置との間で共有する時変情報である第３の情報に基づいて暗号鍵を生成し、上記暗号鍵を用いてデータを暗号化し、暗号化したデータに上記複製制御情報及び時変情報に基づく制御情報を付加した送信データを送信し、データ受信装置において、上記データ送信装置から送られてくる制御情報が付加され暗号化されたデータを受信し、上記データ送信装置との間で秘密に共有されている第１の情報と、上記受信データの制御情報から導かれる第２の情報と、上記データ送信装置との間で共有する時変情報である第３の情報に基づいて暗号鍵を生成し、上記暗号鍵を用いて上記受信データを復号する。

また、本発明に係るデータ送信装置は、データ受信装置との間で秘密に共有されている第１の情報と、データの複製制御情報から導かれる第２の情報と、上記データ受信装置との間で共有する時変情報である第３の情報に基づいて暗号鍵を生成し、この暗号鍵を用いてデータを暗号化する暗号化処理手段と、この暗号化処理手段により暗号化したデータに上記複製制御情報及び時変情報に基づく制御情報を付加した送信データを送信する送信手段とを備える。

また、本発明に係るデータ送信方法では、データ受信装置との間で秘密に共有されている第１の情報と、データの複製制御情報から導かれる第２の情報と、上記データ受信装置との間で共有する時変情報である第３の情報に基づいて暗号鍵を生成し、この暗号鍵を用いてデータを暗号化し、暗号化したデータに上記複製制御情報及び時変情報に基づく制御情報を付加した送信データを送信する。

BNSDOCID: <WO___0062476A1_I_>

また、本発明に係るデータ受信装置は、データ送信装置から送られてくる複製制御情報及び時変情報に基づく制御情報が付加され暗号化されたデータを受信する受信手段と、この受信手段により受信された受信データについて、上記データ送信装置との間で秘密に共有されている第１の情報と、上記受信データの制御情報から導かれる第２の情報と、上記データ送信装置との間で共有する時変情報である第３の情報に基づいて暗号鍵を生成し、上記暗号鍵を用いて上記受信データを復号する復号処理手段とを備える。

さらに、本発明に係るデータ受信方法では、データ送信装置から送られてくる複製制御情報及び時変情報に基づく制御情報が付加され暗号化されたデータを受信し、この受信データについて、上記データ送信装置との間で秘密に共有されている第１の情報と、上記受信データの制御情報から導かれる第２の情報と、上記データ送信装置との間で共有する時変情報である第３の情報に基づいて暗号鍵を生成し、上記暗号鍵を用いて上記受信データを復号する。

図面の簡単な説明

図１は、複製制御情報改竄攻撃による影響を説明するための図である。

図２は、本発明を適用したデータ伝送システムの構成を示すブロック図である。

図３は、ＩＥＥＥ１３９４シリアルバス上を伝送される伝送フレーム（アイソクロナス・パケット）の構成を示す図である。

RNSDOCID: <WO 0062476A1 I >

図４は、上記データ伝送システムにおける認証・鍵共有プロトコルの実行手順を示すフローチャートである。

図５は、上記認証・鍵共有プロトコルにおけるデータ送信装置側の処理手順を示すフローチャートである。

図６は、上記認証・鍵共有プロトコルにおけるデータ受信装置側の処理手順を示すフローチャートである。

図７は、上記データ伝送システムにおけるデータ伝送処理の手順を示すフローチャートである。

図８は、上記データ伝送処理におけるデータ受信装置側の処理手順を示すフローチャートである。

図９は、上記データ伝送処理におけるデータ受信装置側の処理手順を示すフローチャートである。

発明を実施するための最良の形態

以下、本発明を実施するための最良の形態について図面を参照しながら詳細に説明する。

本発明は、例えば図２に示すような構成のデータ伝送システムに適用される。

このデータ伝送システムは、データ送信装置１０とデータ受信装置２０を備え、データ送信装置１０とデータ受信装置２０が伝送路３０を介して接続された構成となっている。

この実施の形態のデータ伝送システムにおいて、データ送信装置１０は、例えば、通信衛星から送られてくる衛星デジタル多チャネ

BNSDOCID: <WO___0062476A1_I_>

ル放送番組を受信するセットトップボックスであって、内部バス１１に接続された中央演算処理ユニット(CPU: Central Processing Unit)１２、メモリ１３、入力インターフェース１４、ユーザインターフェース１５、入出力インターフェース１６等により構成されている。入力インターフェース１４には衛星アンテナ１８が接続されている。また、入出力インターフェース１６は、デジタルインターフェースであるＩＥＥＥ(The International of Electrical and Electronics Engineers,Inc.)１３９４ハイ・パフォーマンス・シリアル・バス・インターフェース（以下、単にＩＥＥＥ１３９４インターフェースという）であって、上記伝送路３０に接続されている。伝送路３０は、ＩＥＥＥ１３９４シリアルバスで構成される伝送路である。

このデータ送信装置１０において、ＣＰＵ１２は、メモリ１３に記憶されている制御プログラムにしたがって動作して、ユーザインターフェース１５を介して入力される操作情報に応じて番組の選局動作等の各種制御動作を行うようになっている。

そして、このデータ送信装置１０は、上記受信アンテナ１８が接続された入力インターフェース１４により衛星デジタル多チャネル放送信号の所望のチャンネルを選局して所望のチャンネルの映像データや音楽データを受信し、受信した映像データや音楽データをコンテンツデータとして入出力インターフェース１６から上記伝送路３０に送信する。

また、データ受信装置２０は、データ送信装置１０により受信したコンテンツデータ、すなわち映像データや音楽データを磁気テープや光磁気ディスクなどの記録媒体に記録する記録装置であって、

内部バス２１に接続された中央演算処理ユニット(CPU: Central Processing Unit)２２、メモリ２３、入出力インターフェース２４、ユーザインターフェース２５、メディアアクセス部２６等により構成されている。入出力インターフェース２４は、デジタルインターフェースであるＩＥＥＥ１３９４インターフェースであって、伝送路３０が接続されている。

ＩＥＥＥ１３９４規格では、ネットワーク内で行われる伝送動作をサブアクションと呼び、次の２種類のサブアクションが規定されている。すなわち、２つのサブアクションとして、「アシンクロナス(Asynchronous) データ転送 」と呼ばれる通常のデータ伝送を行う非同期伝送モード及び、「アイソクロナス(Isochronous) データ転送」と呼ばれる伝送帯域を保証した同期伝送モードが定義されている。

このデータ伝送システムでは、伝送帯域を確保できるIsochronous データ転送を用いて音楽データをデータ送信装置１０とデータ受信装置２０との間で伝送する。

ここで、伝送路３０であるＩＥＥＥ１３９４シリアルバス上をIsochronous転送で伝送されるパケット（アイソクロナス・パケット）の構成を図３に示す。

すなわち、アイソクロナス・パケットは、図３に示すように、ヘッダ、ヘッダＣＲＣ、データフィールド及びデータＣＲＣで構成される。

ヘッダは、データ長(data_length)、タグ(tag)、チャンネル(channel)、ｔコード(tcode)、複製制御情報、Ｏｄｄ／Ｅｖｅｎビット及び同期コードsyを含んでいる。

BNSDOCID: <WO__0062476A1_I_>

データ長(data_length)は、データフィールドの長さを示す。タグ(tag)は、アイソクロナス・パケットが伝送するデータのフォーマットを示す。チャンネル(channel)は、ＩＥＥＥ１３９４シリアルバス上で伝送される複数のアイソクロナス・パケットから所定の所望のパケットの識別を行い、受信するために用いられる。ｔコード(tcode)は、トランザクション・コードであり、アイソクロナス転送であることを示す値が入る。Ｏｄｄ／Ｅｖｅｎビットは、コンテンツキーをＫｃを計算する元ととなる情報の一つである時変情報を与える。複製制御情報は、コンテンツデータの複製の可否を示す。同期コードsyは、送信側と受信側で同期情報をやり取りするのに用いられ、映像データ及び音声データなどのデータフィールドに格納されたコンテンツデータの同期を取るのに使用される。

ヘッダＣＲＣは、ヘッダに格納されたデータに対するＣＲＣ（Cyclic Redundancy Code）の格納される領域である。これに基づいてヘッダの伝送エラーのチェックが行われる。

データフィールドは、映像データや音声データ等のコンテンツデータが格納されるフィールドである。

データＣＲＣは、データフィールドに格納されたデータに対するＣＲＣ（Cyclic Redundancy Code）の格納される領域である。これに基づいてデータの伝送エラーのチェックが行われる。

そして、データ受信装置２０は、入出力インターフェース２４を介してコンテンツデータを受信し、それが記録可能であれば、メディアアクセス部２６により磁気テープや光磁気ディスクなどの記録媒体に記録する。

また、データ受信装置２０は、記録禁止のコンテンツデータを受

信した場合には、メディアアクセス部２６により記録媒体に記録することなく、単に、音楽データを音声出力端子２６Ａから出力し、また映像データを映像出力端子２６Ｂから出力する。

このデータ受信装置２０において、ＣＰＵ２２は、メモリ２３に記憶されている制御プログラムにしたがって動作して、ユーザインターフェース２５を介して入力される操作情報に応じて、記録媒体に対してメディアアクセス部２６による記録する動作及び再生する動作等の各種制御動作を行うようになっている。

このデータ伝送システムおいて、コンテンツデータは、次のようにして、暗号鍵（コンテンツキーＫｃ）により暗号化されてアイソクロナス・パケットのデータフィールドに格納され、そのアイソクロナス・パケットのヘッダに格納される時変情報（時変値Ｎｃ）を与えるＯｄｄ／Ｅｖｅｎビットとコンテンツデータの複製の可否を示す複製制御情報とともに伝送される。

すなわち、データ伝送システムを構成するデータ送信装置１０及びデータ受信装置２０は、それぞれ固有又は共通の秘密情報を予め持っている。すなわち、公開鍵方式の場合には固有の秘密情報を持ち、共通鍵方式の場合は共通の秘密情報を持つ。例えば、各機器が製造される際に鍵管理機関から与えられる機器用の鍵を機器内にもっている。ここでは、機器用の鍵として共通の秘密情報を持っているものとする。また、各機器は、鍵管理機関から与えられる複製制御情報のそれぞれのステートに対応するｎ（例えばｎ＝６４）ビットの定数を機器内に保存している。すなわち、各機器は、もともとコピー禁止を表す複製制御情報「１１」(Copy-never)に対応する定数Ｃａ、一世代のみコピー可を表す複製制御情報「１０」(Copy-on

BNSDOCID: <WO___0062476A1_I_>

e-generation)に対応する定数Ｃｂ、“Copy-one-generation”だったコンテンツが一度記録されたコンテンツであることを表し、これ以上のコピー禁止を表す複製制御情報「０１」(No-more-copies)に対応する定数Ｃｃ、及び、コピー制限なしを表す複製制御情報「００」(Copy-freely)に対応する定数Ｃｄをもっている。

データ送信装置１０は、データを送信するに当たり、例えばｍビットの乱数を２つ生成し、一方を認証・鍵共有プロトコルの実行の際にデータ受信装置２０に送られるエクスチェンジキーＫｘとし、他方をデータ伝送の際に使用する時変値Ｎｃの初期値とする。エクスチェンジキーＫｘは、コンテンツキーＫｃを計算する元となる情報の一つであって、認証・鍵共有プロトコルにより共有された鍵を用いてデータ送信装置１０からデータ受信装置２０に送られる。そして、データを送信する際に、そのデータに応じて複製制御情報をパケットヘッダに書き込む。次に、エクスチェンジキーＫｘと時変値Ｎｃ（アイソクロナス・パケットのヘッダに格納される時変情報）と複製制御情報を用いて、コンテンツキーＫｃを計算し、コンテンツキーＫｃを用いてデータを暗号化して、アイソクロナス・パケットのデータフィールドに格納して、パケットヘッダと共に伝送路に送信する。

コンテンツキーＫｃは、例えば複製制御情報が「１０」であるとき、例えば次のように、

Ｋｃ＝Ｊ［Ｋｘ，Ｎｃ，Ｃｂ］

にて計算する。

ここで、関数Ｊは、出力から入力を求めることが困難な関数（一方向関数）である。関数Ｊの具体例としては、例えばＦＩＰＳ(Fed

eral Information Processing Standard)１８０－１のＳＨＡ(Secure Hash Algorithm)－１を用いることができ、また、ＤＥＳ(Data Encryption Standard)等のブロック暗号を用いて構成することも可能である。

ＳＨＡ－１を用いた場合、ＳＨＡ－１にＫｘ，Ｎｃ，Ｃｂのビット連結（Ｋｘ‖Ｎｃ‖Ｃｂ）を入力する。なお、必要に応じて関数Ｊの出力（例えばＳＨＡ－１を用いた場合には１６０ビット）を、暗号アルゴリズムの鍵ビット数（例えばＤＥＳの場合には５６ビット）に拡大、縮小してコンテンツキーＫｃとするようにしてもよい。拡大する場合には、例えば出力を複数回繰り返し並べれば良く、縮小するには、上位あるいは下位の必要ビット数だけを使用する。

ＤＥＳやＳＨＡ－１などの暗号技術については、Bruce Schneier著「Applied Cryptography(Second Edition),Wiley」に詳しく解説されている。

さらに、データ送信装置１０は、時変値Ｎｃに応じて、データパケットのＯｄｄ／Ｅｖｅｎビットの値をセットする。例えば時変値Ｎｃの最下位ビットとＯｄｄ／Ｅｖｅｎビットの値が一致するようにセットする。ここで、データ送信装置１０は、例えば３０秒以上２分以内など時間条件により、あるいは、伝送開始又は前回の更新から送信したデータのパケット数やバイト数等のデータ量の条件により、時変値Ｎｃを更新する。時変値Ｎｃの更新は、所定の時間間隔もしくは送信量をタイミングとしてインクリメントすることにより行う。そして、時変値Ｎｃの更新に応じて新たにコンテンツキーＫｃを計算し、このコンテンツキーＫｃでコンテンツを暗号化してパケットに格納する。また、データパケットのＯｄｄ／Ｅｖｅｎビ

BNSDOCID: <WO___0062476A1_I_>

ットの値を変化させる。

このデータ伝送システムでは、上記データ伝送に先立って、データ送信装置１０とデータ受信装置２０の間で互いの機器の認証と暗号鍵を共有するためのプロトコルを実行する。具体的には、図４のフローチャートに示すような認証・鍵共有プロトコルを実行してから、データ伝送を行う。なお、このデータ伝送システムにおけるデータ送信装置１０側の処理手順を図５のフローチャートに示すとともに、データ受信装置２０側の処理手順を図６のフローチャートに示す。

ここで、この認証・鍵共有プロトコルを示す図４では、データ送信装置１０をSource DeviceAで表し、データ受信装置２０をSink DeviceBで表す。

そして、このデータ伝送システムおいて、データ送信装置１０のＣＰＵ１２は、先ず、データの伝送を開始するためのスタートコマンドを上記入出力インターフェース１６から伝送路３０を介してデータ受信装置２０に送信する（ステップＳ１０）。

データ受信装置２０のＣＰＵ２２は、入出力インターフェース２４に接続された上記伝送路３０を介して上記データ送信装置１０から送られてくるスタートコマンド(START command) を受信したら（ステップＳ２０）、m（例えばm＝６４）ビットの乱数R_B を生成し、この乱数R_B とデータ受信装置２０の識別子ID_B のビット連結（$R_B \| ID_B$）を認証・鍵共有プロトコルの開始要求(Request authentication)共にデータ送信装置１０に入出力インターフェース２４を介して送信する（ステップＳ２１）。

データ送信装置１０のＣＰＵ１２は、入出力インターフェース１

６に接続された伝送路３０を介してデータ受信装置２０から送られてくる認証・鍵共有プロトコルの開始要求(Request authentication)とビット連結（$R_B \| ID_B$）を受信したら（ステップＳ１１）、ｍビットの乱数R_Aを生成し、

$$TokenAB = RA \| MAC(K_{AB}, R_A \| R_B \| ID_B)$$

なる演算処理により、第１の認証情報ＴｏｋｅｎＡＢを求め、この第１の認証情報ＴｏｋｅｎＡＢをデータ受信装置２０に入出力インターフェース１６を介して送信する（ステップＳ１２）。ここで、ＭＡＣは、ＩＳＯ／ＩＥＣ　９７９７に記載されている方式で作成されたメッセージ認証コード(Message Authentication Code)である。暗号関数としてはＤＥＳを使用する。また、K_{AB}は、データ送信装置１０とデータ受信装置２０の間で共有されている秘密情報である。すなわち、K_{AB}は、上述のように鍵管理機関から与えられた機器用の鍵である。

データ受信装置２０のＣＰＵ２２は、データ送信装置１０から第１の認証情報ＴｏｋｅｎＡＢを受け取ったら（ステップＳ２２）、K_{AB}, R_A, R_B, ID_Bを用いて独自にＭＡＣを計算し（ステップＳ２３）、受信したものと一致することを確認する（ステップＳ２４）。このステップＳ２４において一致しなければ、データ受信装置２０のＣＰＵ２２は、データ送信装置１０が不正な機器であると判断して、この認証・鍵共有プロトコルを終了する。

次に、データ受信装置２０のＣＰＵ２２は、ｍビットの乱数Ｓを生成し、

$$TokenBA = S \| MAC(K_{AB}, R_B \| R_A)$$

なる演算処理により、第２の認証情報ＴｏｋｅｎＢＡを求め、この

BNSDOCID: <WO___0062476A1_I_>

第２の認証情報ＴｏｋｅｎＢＡをデータ送信装置１０に入出力インターフェース２４を介して送る（ステップＳ２５）。なお、上記乱数Ｓは、上記乱数R_Bと同じｍビットでなくてもよい。ここで、データ受信装置２０のＣＰＵ２２は、ＭＡＣ（K_{AB}，Ｓ）の上位ｍビットを後述する一時キーとして使用する。

データ送信装置１０のＣＰＵ１２は、データ受信装置２０から第２の認証情報ＴｏｋｅｎＢＡを受け取ったら（ステップＳ１３）、K_{AB}，R_A，R_Bを用いて独自にＭＡＣを計算し（ステップＳ１４）、受信したものと一致することを確認する（ステップＳ１５）。このステップＳ１５において、一致しなければ、データ送信装置１０のＣＰＵ１２は、データ受信装置２０が不正な機器であると判断して、この認証・鍵共有プロトコルを終了する。そして、このステップＳ４において、一致したら、データ送信装置１０のＣＰＵ１２は、データ受信装置２０を正当な機器であると認証し、ＭＡＣ（K_{AB}，Ｓ）の上位ｍビットを後述する一時キーとして使用する。

なお、ＭＡＣ（K_{AB}，Ｓ）の上位ｍビットを一時キーとして使用するが、そのビット数は、乱数Ｓと同じのビット数ｍと同じである必要はない。

次に、データ送信装置１０のＣＰＵ１２は、エクスチェンジキーＫｘを例えばＤＥＳ暗号関数を用いて一時キーで暗号化し、暗号化したエクスチェンジキーＫｘをデータ受信装置２０に入出力インターフェース１６を介して送信する（ステップＳ１６）。

そして、データ受信装置２０は、データ送信装置１０から送られてきた暗号化されたエクスチェンジキーＫｘをＤＥＳ復号関数を用いて一時キーで復号して、エクスチェンジキーＫｘを得る（ステッ

UNSDOCID: <WO 0062476A1_I_>

プＳ２６）。

このデータ伝送システムにおけるデータ受信装置２０は、データ送信装置１０との間で認証・鍵共有プロトコルを実行することにより得たエクスチェンジキーＫｘ及び時変値Ｎｃ、データパケットの複製制御情報に対応した定数（この例ではＣｂ）から、コンテンツキーＫｃをデータ送信装置１０と同様に計算することができ、このコンテンツキーＫｃを用いてデータを復号することができるようになる。

このデータ伝送システムでは、上記認証・鍵共有プロトコルを実行してから、図７のフローチャートに示すような手順に従ってデータ伝送を行う。このデータ伝送システムにおけるデータ受信装置２０側の処理手順を図８のフローチャートに示すとともに、データ送信装置１０側の処理手順を図９のフローチャートに示す。

すなわち、上記認証・鍵共有プロトコルによりエクスチェンジキーＫｘを得たデータ受信装置２０のＣＰＵ２２は、次に、データ送信装置１０に対し、現在の時変値Ｎｃを送るように要求する（ステップＳ３０）。

データ送信装置１０のＣＰＵ１２は、このＮｃ要求を受信すると（Ｓ４０）、この要求に応じて現在の時変値Ｎｃを上記データ受信装置２０に送信し（ステップＳ４１）、この時変値Ｎｃをデータ受信装置２０が受信する（ステップＳ３１）。

データ受信装置２０は、データ送信装置１０から送られてきた時変値Ｎｃの最下位ビットとデータパケット中のＯｄｄ／Ｅｖｅｎビットが等しいことを確認し、等しい場合に、時変値Ｎｃとエクスチェンジキーｋｘ、定数Ｃｂからコンテンツキーｋｃを計算する（ス

DNSDOCID: <WO___0062476A1_I_>

テップＳ３２）。時変値Ｎｃの最下位ビットとデータパケット中のＯｄｄ／Ｅｖｅｎビットが等しくない場合には、データ受信装置２０は、コンテンツキーＫｃが既に更新されたと判断し、送られた時変値Ｎｃをインクリメントした値を新たな時変値Ｎｃとして、コンテンツキーＫｃを計算する。

なお、上記Ｎｃ要求に応じてデータ送信装置１０から時変値Ｎｃをデータ受信装置２０に送った後では、データ送信装置１０及びデータ受信装置２０は、共に、次の時変値Ｎｃの更新後の値が現在の値をインクリメントしたものであることが判っているので、予め次に使われるコンテンツキーＫｃを計算しておくことができる。

次に、データ送信装置１０は、映像データや音声データなどのコンテンツデータを暗号鍵（コンテンツキーＫｃ）で暗号化し、暗号化したコンテンツデータをアイソクロナス・パケットのデータフィールドに格納し、そのアイソクロナス・パケットのヘッダに格納される時変情報を与えるＯｄｄ／Ｅｖｅｎビット及びコンテンツデータの複製制御情報とともに順次送信する（ステップＳ４２，Ｓ４３）。

すなわち、データ送信装置１０では、例えば時変値Ｎｃに応じたＯｄｄ／Ｅｖｅｎビットの設定状態を判定して（ステップＳ４１Ａ）、Ｏｄｄ／Ｅｖｅｎビット＝０であれば、Ｏｄｄ／Ｅｖｅｎビット＝０に対応するコンテンツキーＫｃ（Ｏｄｄキー）でコンテンツデータを暗号化した暗号化データを送信し（ステップＳ４２）、また、Ｏｄｄ／Ｅｖｅｎビット＝１であれば、Ｏｄｄ／Ｅｖｅｎビット＝１に対応するコンテンツキーＫｃ（Ｅｖｅｎキー）でコンテンツデータを暗号化した暗号化データを送信する処理を行う（ステ

BNSDOCID: <WO__0062476A1_I_>

ップＳ４３）。そして、送信終了か否かを判定し（ステップＳ４４）、その判定結果がＮＯすなわち送信終了でなければ、時変値Ｎｃの更新タイミングになったか否かを判定し（ステップＳ４５）、更新タイミングでなければ時変値Ｎｃを更新することなく上記Ｏｄｄ／Ｅｖｅｎビットの設定状態の判定処理（ステップＳ４１Ａ）に戻り、更新タイミングになったら時変値Ｎｃをインクリメントすることにより更新するとともにＯｄｄ／Ｅｖｅｎビットを更新し（ステップＳ４６）、上記Ｏｄｄ／Ｅｖｅｎビットの設定状態の判定処理（ステップＳ４１Ａ）に戻ることにより、上記Ｏｄｄ／Ｅｖｅｎビット＝０に対応するコンテンツキーＫｃ（Ｏｄｄキー）でコンテンツデータを暗号化した暗号化データの送信処理（ステップＳ４２）と、Ｏｄｄ／Ｅｖｅｎビット＝１に対応するコンテンツキーＫｃ（Ｅｖｅｎキー）でコンテンツデータを暗号化した暗号化データの送信処理（ステップＳ４３）を繰り返し行う。

そして、上記送信終了か否かの判定処理（ステップＳ４４）のＹＥＳすなわち送信終了であれば、データ伝送モードの処理を終了する。

データ受信装置２０は、このようにしてデータ送信装置１０から送られてくる暗号化データを受信すると、計算したコンテンツキーＫｃを用いてデータを復号する（ステップＳ３３，Ｓ３４）。

すなわち、データ受信装置２０では、暗号化データの受信受信復号処理（ステップＳ３３，Ｓ３４）を行う毎に、受信終了か否かを判定し（ステップＳ３５）、その判定結果がＮＯすなわち受信終了でなければ、時変値Ｎｃの更新タイミングになったか否かを判定し（ステップＳ３６）、更新タイミングでなければ時変値Ｎｃを更新

BNSDOCID: <WO___0062476A1_I_>

することなく上記コンテンツキーＫｃの計算処理（ステップＳ３２）に戻り、更新タイミングになったら時変値Ｎｃをインクリメントすることにより更新して（ステップＳ３７）、上記コンテンツキーＫｃの計算処理（ステップＳ３２）に戻ることにより、上記Ｏｄｄ／Ｅｖｅｎビット＝０に対応する暗号化データの受信復号処理（ステップＳ３３）と、上記Ｏｄｄ／Ｅｖｅｎビット＝１に対応する暗号化データの受信送信処理（ステップＳ３４）を繰り返し行う。

データ受信装置２０は、計算したコンテンツキーＫｃを用いてデータを復号することにより、このデータパケットに格納されていた複製制御情報に応じて、データの記録を可能にしたり禁止したりする制御を行うことができる。

なお、上述の実施の形態では、データ受信装置１０が１台のデータ伝送システムについて説明したが、複数台のデータ受信装置がある場合にも、本発明は、そのまま適用することができる。

このような構成のデータ伝送システムにおいて、例えば、データ送信装置１０側からデータパケットのパケットヘッダの複製制御情報をコピー禁止の意味表す「１１」で送信した場合に、伝送中に複製制御情報改竄攻撃があり、複製制御情報が１回コピー可を表す「１０」に改竄されてしまうと、このパケットを受信したデータ受信装置２０側では、このデータの複製制御情報「１０」に対応した定数Ｃｂを用いてコンテンツキーＫｃを計算し、このコンテンツキーＫｃを用いてコンテンツデータを復号することになる。

データ送信装置１０側におけるコンテンツデータの暗号化は、複製制御情報「１１」に対応した定数Ｃａを用いて計算したコンテンツキーＫｃにより行われているので、データ受信装置２０側におい

BNSDOCID: <WO 0062476A1 I >

て復号の結果として得られるデータは無意味なデータとなる。すなわち、データ受信装置２０で現れるデータは、元のコンテンツデータではないので記録しても意味がなく、コピーの世代管理が崩れることはない。

また、このデータ伝送システムでは、コンテンツキーＫｃに時変値Ｎｃを作用させているので、この時変値Ｎｃを頻繁に変えることにより、同一の暗号鍵を用いて暗号化されるデータの量を制限することができ、暗号解析のおそれを少なくすることができる。

さらに、時変値Ｎｃの更新をインクリメントにより行い、現在使われている時変値に対応した値をデータパケットに格納して伝送することにより、データ受信装置２０側で時変値Ｎｃの更新を簡単に知ることができ、また、正しいコンテンツキーＫｃをデータ送信装置１０及びデータ受信装置２０が共に予め計算しておくことができる。これにより、時変値Ｎｃの更新がある毎に、データ受信装置２０がデータ送信装置１０対して時変値Ｎｃを問い合わせる必要もなく、システム全体としての通信量の抑制、制御ソフトウエアの簡略化を図ることができる。

また、コンテンツキーＫｃを計算する際に、出力から入力を求めることが困難な一方向性関数を用いているので、仮に上記コンテンツキーＫｃが露見したとしても、エクスチェンジキーＫｘや複製制御情報に対応する定数が不正に求められてしまうことがない。したがって、あるコンテンツキーＫｃが露見したとしても、別のコンテンツキーＫｃを用いて暗号化されたコンテンツデータが解読されてしまうことはない。

以上のように本発明の実施の形態においては、データ送信装置か

BNSDOCID: <WO__ 0062476A1_I_>

らデータ受信装置にデータを一方伝送するに当たり、データ受信装置との間で秘密に共有されている第１の情報と、送信データの複製制御情報から導かれる第２の情報と、上記データ受信装置との間で共有する時変情報である第３の情報によって暗号鍵を生成し、この暗号鍵を用いてデータを暗号化し、暗号化したデータに上記複製制御情報及び時変情報を付加した送信データをデータ送信装置から送信することにより、データ受信装置側では、上記データ送信装置から送られてくる複製制御情報及び時変情報が付加され暗号化されたデータを受信し、受信された受信データについて、上記データ送信装置との間で秘密に共有されている第１の情報と、上記受信データの複製制御情報から導かれる第２の情報と、上記データ送信装置との間で共有する時変情報である第３の情報によって暗号鍵を生成し、この暗号鍵を用いて上記受信データを復号することができる。

このように送信データの暗号鍵に上記送信データの複製制御情報から導かれる第２の情報を暗号鍵に作用させておくことにより、伝送中に複製制御情報改竄攻撃によって複製制御情報が改竄されてしまった場合には、データ再生装置側で受信したデータの複製制御情報に応じた第２の情報に基づいて計算される暗号鍵はデータ送信装置側で使用した暗号鍵とは異なるものとなるので、受信データを正常に復号することができず、コピーの世代管理が崩れることはない。

また、暗号鍵に時変情報を作用させているので、この時変情報を頻繁に変えることにより、同一の暗号鍵を用いて暗号化されるデータの量を制限することができ、暗号解析のおそれを少なくすることができる。

さらに、時変情報の更新をインクリメントにより行い、現在使わ

BNSDOCID: <WO 0062476A1 I >

れている時変情報に対応した値をデータパケットに格納して伝送することにより、データ受信装置側で時変情報の更新を簡単に知ることができ、また、正しい暗号鍵をデータ送信装置及びデータ受信装置が共に予め計算しておくことができる。これにより、時変情報の更新がある毎に、データ受信装置がデータ送信装置１０対して時変値Ｎｃを問い合わせる必要もなく、システム全体としての通信量の抑制、制御ソフトウエアの簡略化を図ることができる。

また、上記暗号鍵を計算する際に、出力から入力を求めることが困難な一方向性関数を用いることにより、仮に上記暗号鍵が露見したとしても、データ受信装置との間で秘密に共有されている第１の情報や複製制御情報に対応する第２の情報が不正に求められてしまうことがない。したがって、ある暗号鍵が露見したとしても、別の暗号鍵を用いて暗号化されたデータが解読されてしまうことはない。

BNSDOCID: <WO___0062476A1_I_>

請求の範囲

１．　データ受信装置との間で秘密に共有されている第１の情報と、データの複製制御情報から導かれる第２の情報と、上記データ受信装置との間で共有する時変情報である第３の情報に基づいて暗号鍵を生成し、上記暗号鍵を用いてデータを暗号化し、暗号化したデータに上記複製制御情報及び時変情報に基づく制御情報を付加した送信データを送信するデータ送信装置と、

上記データ送信装置から送られてくる制御情報が付加され暗号化されたデータを受信し、上記データ送信装置との間で秘密に共有されている第１の情報と、上記受信データの制御情報から導かれる第２の情報と、上記データ送信装置との間で共有する時変情報である第３の情報に基づいて暗号鍵を生成し、上記暗号鍵を用いて上記受信データを復号するデータ受信装置とからなるデータ伝送システム。

２．　上記データ送信装置及びデータ受信装置は、それぞれ上記第３の情報として予め定められた時間条件により変動する時変情報を用いて、上記暗号鍵を生成する請求の範囲第１項記載のデータ伝送システム。

３．　上記データ送信装置及びデータ受信装置は、それぞれ上記第３の情報として予め定められたデータ量の条件により変動する時変情報を用いて、上記暗号鍵を生成する請求の範囲第１項記載のデータ伝送システム。

４．　上記データ送信装置及びデータ受信装置は、それぞれ上記第３の情報として変動前の値を用いて変動後の値を求めることが可能

BNSDOCID: <WO___0062476A1_I_>

な時変情報を用いて、上記暗号鍵を生成する請求の範囲第１項記載のデータ伝送システム。

５．　上記データ受信装置は、上記受信データに付加された制御情報に基づいて上記時変情報である第３の情報の変化を検出し、上記第３の情報を更新する請求の範囲第４項記載のデータ伝送システム。

６．　上記データ受信装置は、上記受信データに付加された制御情報に基づいて上記時変情報である第３の情報の変化を検出し、更新前の上記第３の情報に対してインクリメント処理を施した値に基づいて更新された第３の情報を算出する請求の範囲第５項記載のデータ伝送システム。

７．　上記データ送信装置及びデータ受信装置は、それぞれ一方向関数を用いて、上記第１の情報と第２の情報と第３の情報から上記暗号鍵を生成する請求の範囲第１項記載のデータ伝送システム。

８．　暗号化されたデータを復号する装置で復号処理される伝送信号であって、

データの複製の許可状態を示す複製許可情報と、所定時間毎に更新される時変情報とを具備するヘッダと、

上記複製許可情報と上記時変情報とに基づく暗号鍵を用いて暗号化されたデータとを具備する伝送信号。

９．　データ送信装置とデータ受信装置の間で秘密に共有されている第１の情報と、送信データの複製制御情報から導かれる第２の情報と、データ受信装置との間で共有する時変情報である第３の情報によって生成された暗号鍵を用いてデータを暗号化して伝送するデータ伝送方法。

１０．　上記第３の情報として予め定められた時間条件により変動

BNSDOCID: <WO__0062476A1_I_>

する時変情報を用いて、上記暗号鍵を生成する請求の範囲第９項記載のデータ伝送方法。

１１．　上記第３の情報として予め定められたデータ量の条件により変動する時変情報を用いて、上記暗号鍵を生成する請求の範囲第９項記載のデータ伝送方法。

１２．　上記第３の情報として変動前の値を用いて変動後の値を求めることが可能な時変情報を用いて、上記暗号鍵を生成する請求の範囲第９項請求項記載のデータ伝送方法。

１３．　一方向関数を用いて、上記第１の情報と第２の情報と第３の情報から上記暗号鍵を生成する請求の範囲第９項記載のデータ伝送方法。

１４．　データ送信装置において、データ受信装置との間で秘密に共有されている第１の情報と、データの複製制御情報から導かれる第２の情報と、上記データ受信装置との間で共有する時変情報である第３の情報に基づいて暗号鍵を生成し、上記暗号鍵を用いてデータを暗号化し、暗号化したデータに上記複製制御情報及び時変情報に基づく制御情報を付加した送信データを送信し、

データ受信装置において、上記データ送信装置から送られてくる制御情報が付加され暗号化されたデータを受信し、上記データ送信装置との間で秘密に共有されている第１の情報と、上記受信データの制御情報から導かれる第２の情報と、上記データ送信装置との間で共有する時変情報である第３の情報に基づいて暗号鍵を生成し、上記暗号鍵を用いて上記受信データを復号するデータ伝送方法。

１５．　上記データ送信装置及びデータ受信装置において、それぞれ上記第３の情報として予め定められた時間条件により変動する時

RNSDOCID: <WO 0062476A1 | >

変情報を用いて、上記暗号鍵を生成する請求の範囲第１４項記載のデータ伝送方法。

１６．　上記データ送信装置及びデータ受信装置において、それぞれ上記第３の情報として予め定められたデータ量の条件により変動する時変情報を用いて、上記暗号鍵を生成する請求の範囲第１４項記載のデータ伝送方法。

１７．　上記データ送信装置及びデータ受信装置において、それぞれ上記第３の情報として変動前の値を用いて変動後の値を求めることが可能な時変情報を用いて、上記暗号鍵を生成する請求の範囲第１４項記載のデータ伝送方法。

１８．　上記データ受信装置において、上記受信データに付加された制御情報に基づいて上記時変情報である第３の情報の変化を検出し、上記第３の情報を更新する請求の範囲第１４項記載のデータ伝送方法。

１９．　上記データ受信装置において、上記受信データに付加された制御情報に基づいて上記時変情報である第3の情報の変化を検出し、更新前の上記第３の情報に対してインクリメント処理を施した値に基づいて更新された第３の情報を算出する請求の範囲第１８項記載のデータ伝送方法。

２０．　上記データ送信装置及びデータ受信装置において、それぞれ一方向関数を用いて、上記第１の情報と第２の情報と第３の情報から上記暗号鍵を生成する請求の範囲第１４項記載のデータ伝送方法。

２１．　データ受信装置との間で秘密に共有されている第１の情報と、データの複製制御情報から導かれる第２の情報と、上記データ

BNSDOCID: <WO___0062476A1_I_>

受信装置との間で共有する時変情報である第３の情報に基づいて暗号鍵を生成し、この暗号鍵を用いてデータを暗号化する暗号化処理手段と、

この暗号化処理手段により暗号化したデータに上記複製制御情報及び時変情報に基づく制御情報を付加した送信データを送信する送信手段と

を備えるデータ送信装置。

２２．　上記暗号化処理手段は、上記第３の情報として予め定められた時間条件により変動する時変情報を用いて生成した暗号鍵により、データを暗号化する請求の範囲第２１項記載のデータ送信装置。

２３．　上記暗号化処理手段は、上記第３の情報として予め定められたデータ量の条件により変動する時変情報を用いて生成した暗号鍵により、データを暗号化する請求の範囲第２１項記載のデータ送信装置。

２４．　上記暗号化処理手段は、上記第３の情報として変動前の値を用いて変動後の値を求めることが可能な時変情報を用いて生成した暗号鍵により、データを暗号化する請求の範囲第２１項記載のデータ送信装置。

２５．　上記暗号化処理手段は、上記第１の情報と第２の情報と第３の情報から一方向関数を用いて生成した暗号鍵により、データを暗号化する請求の範囲第２１項記載のデータ送信装置。

２６．　データ受信装置との間で秘密に共有されている第１の情報と、データの複製制御情報から導かれる第２の情報と、上記データ受信装置との間で共有する時変情報である第３の情報に基づいて暗号鍵を生成し、

BNSDOCID: <WO 0062476A1 I >

この暗号鍵を用いてデータを暗号化し、

暗号化したデータに上記複製制御情報及び時変情報に基づく制御情報を付加した送信データを送信するデータ送信方法。

２７．　上記第３の情報として予め定められた時間条件により変動する時変情報を用いて生成した暗号鍵により、データを暗号化する請求の範囲第２６項記載のデータ送信方法。

２８．　上記第３の情報として予め定められたデータ量の条件により変動する時変情報を用いて生成した暗号鍵により、データを暗号化する請求の範囲第２６項記載のデータ送信方法。

２９．　上記第３の情報として変動前の値を用いて変動後の値を求めることが可能な時変情報を用いて生成した暗号鍵により、データを暗号化する請求の範囲第２６項記載のデータ送信方法。

３０．　上記第１の情報と第２の情報と第３の情報から一方向関数を用いて生成した暗号鍵により、データを暗号化する請求の範囲第２６項記載のデータ送信方法。

３１．　データ送信装置から送られてくる複製制御情報及び時変情報に基づく制御情報が付加され暗号化されたデータを受信する受信手段と、

この受信手段により受信された受信データについて、上記データ送信装置との間で秘密に共有されている第１の情報と、上記受信データの制御情報から導かれる第２の情報と、上記データ送信装置との間で共有する時変情報である第３の情報に基づいて暗号鍵を生成し、上記暗号鍵を用いて上記受信データを復号する復号処理手段と

を備えるデータ受信装置。

３２．　上記復号処理手段は、上記第３の情報として予め定められ

BNSDOCID: <WO__0062476A1_I_>

た時間条件により変動する時変情報を用いて生成した暗号鍵により、上記受信データを復号する請求の範囲第３１項記載のデータ受信装置。

３３．　上記復号処理手段は、上記第３の情報として予め定められたデータ量の条件により変動する時変情報を用いて生成した暗号鍵により、上記受信データを復号する請求の範囲第３１項記載のデータ受信装置。

３４．　上記復号処理手段は、上記第３の情報として変動前の値を用いて変動後の値を求めることが可能な時変情報を用いて生成した暗号鍵により、上記受信データを復号する請求の範囲第３１項記載のデータ受信装置。

３５．　上記復号処理手段は、上記受信データに付加された制御情報に基づいて上記時変情報である第３の情報の変化を検出し、上記第３の情報を更新する請求の範囲第３１項記載のデータ受信装置。

３６．　上記復号処理手段は、上記受信データに付加された制御情報に基づいて上記時変情報である第３の情報の変化を検出し、更新前の上記第３の情報に対してインクリメント処理を施した値に基づいて更新された第３の情報を算出する請求の範囲第３５項記載のデータ受信装置。

３７．　上記暗号化処理手段は、上記第１の情報と第２の情報と第３の情報から一方向関数を用いて生成した暗号鍵により、上記受信データを復号することを特徴とする請求の範囲第３１項記載のデータ受信装置。

３８．　データ送信装置から送られてくる複製制御情報及び時変情報に基づく制御情報が付加され暗号化されたデータを受信し、

この受信データについて、上記データ送信装置との間で秘密に共有されている第１の情報と、上記受信データの制御情報から導かれる第２の情報と、上記データ送信装置との間で共有する時変情報である第３の情報に基づいて暗号鍵を生成し、上記暗号鍵を用いて上記受信データを復号するデータ受信方法。

３９．　上記第３の情報として予め定められた時間条件により変動する時変情報を用いて生成した暗号鍵により、上記受信データを復号する請求の範囲第３８項記載のデータ受信方法。

４０．　上記第３の情報として予め定められたデータ量の条件により変動する時変情報を用いて生成した暗号鍵により、上記受信データを復号する請求の範囲第３８項記載のデータ受信方法。

４１．　上記第３の情報として変動前の値を用いて変動後の値を求めることが可能な時変情報を用いて生成した暗号鍵により、上記受信データを復号する請求の範囲第３８項記載のデータ受信装置。

４２．　上記受信データに付加された制御情報に基づいて上記時変情報である第３の情報の変化を検出し、上記第３の情報を更新する請求の範囲第３８項記載のデータ受信方法。

４３．　上記受信データに付加された制御情報に基づいて上記時変情報である第３の情報の変化を検出し、更新前の上記第３の情報に対してインクリメント処理を施した値に基づいて更新された第３の情報を算出する請求の範囲第４２項記載のデータ受信方法。

４４．　上記第１の情報と第２の情報と第３の情報から一方向関数を用いて生成した暗号鍵により、上記受信データを復号することを特徴とする請求の範囲第３８項記載のデータ受信方法。

BNSDOCID: <WO___0062476A1_I_>

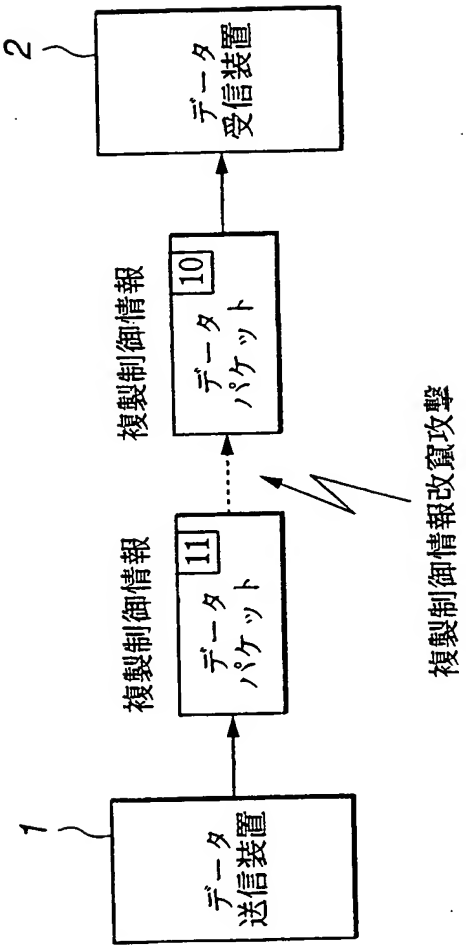

1
データ送信装置
複製制御情報
11
データパケット
2
データ受信装置
複製制御情報
10
データパケット
複製制御情報改竄攻撃

FIG.1

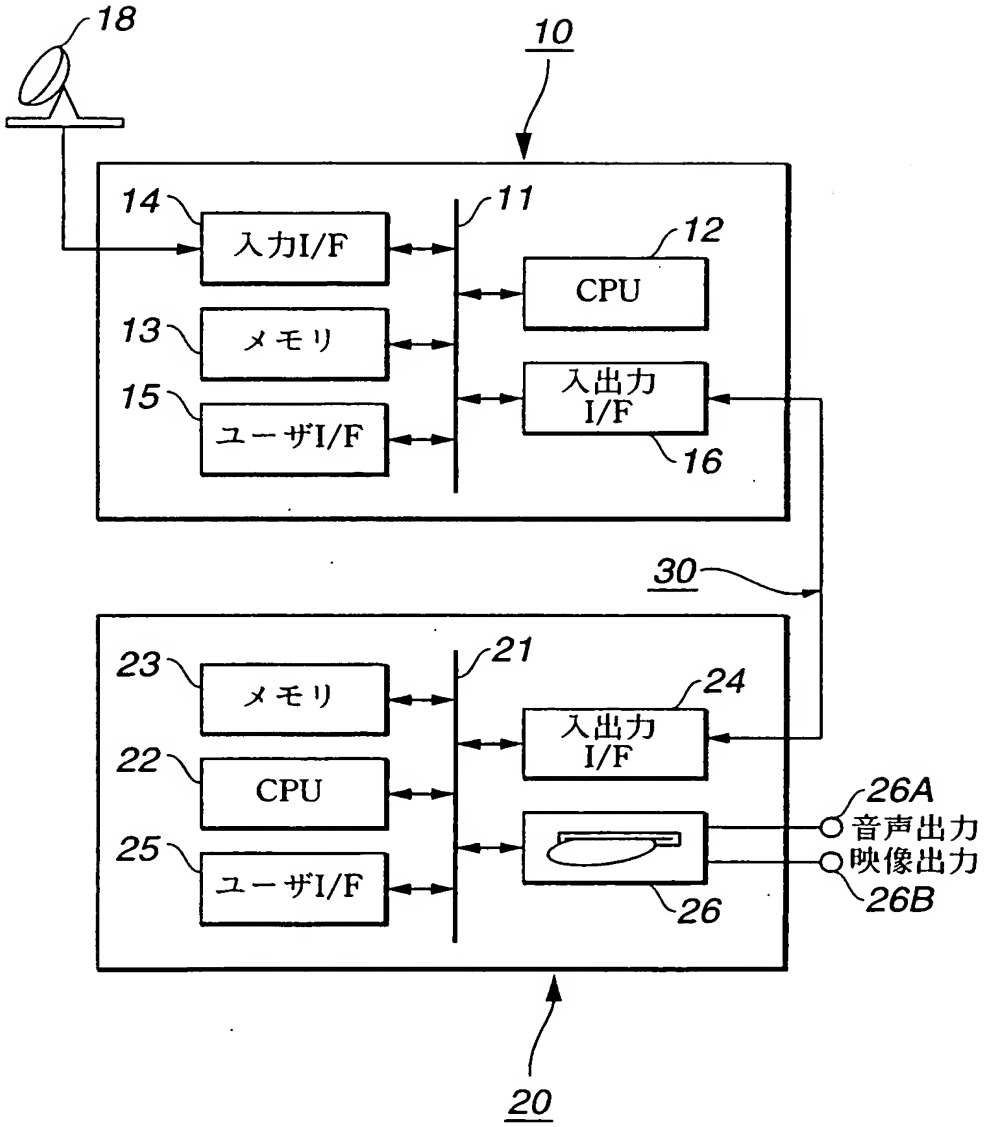

18
10
14
入力I/F
11
12
CPU
13
メモリ
15
ユーザI/F
入出力
I/F
16
30
23
メモリ
21
24
入出力
I/F
22
CPU
26A
音声出力
映像出力
25
ユーザI/F
26
26B
20

FIG.2

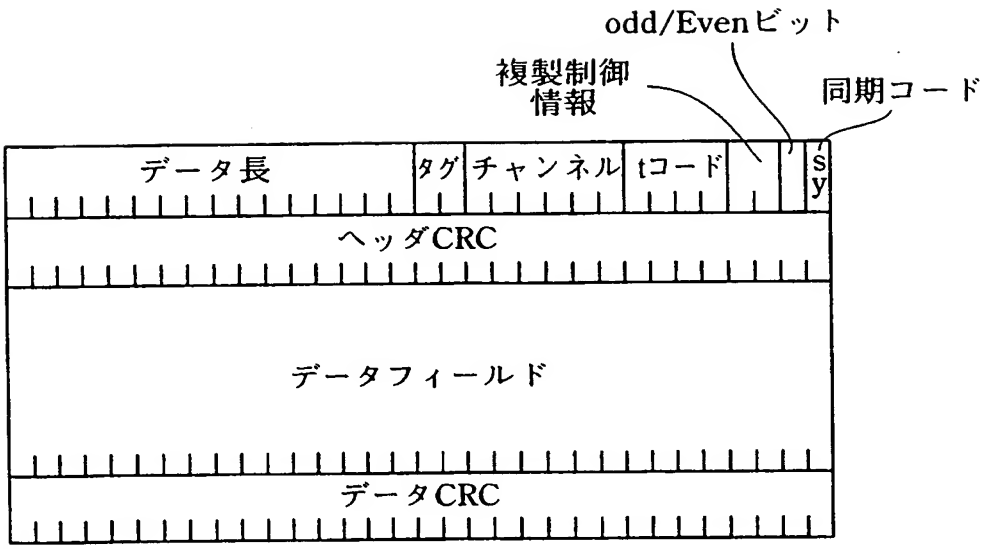


FIG.3

BNSDOCID: <WO___0062476A1_I_>

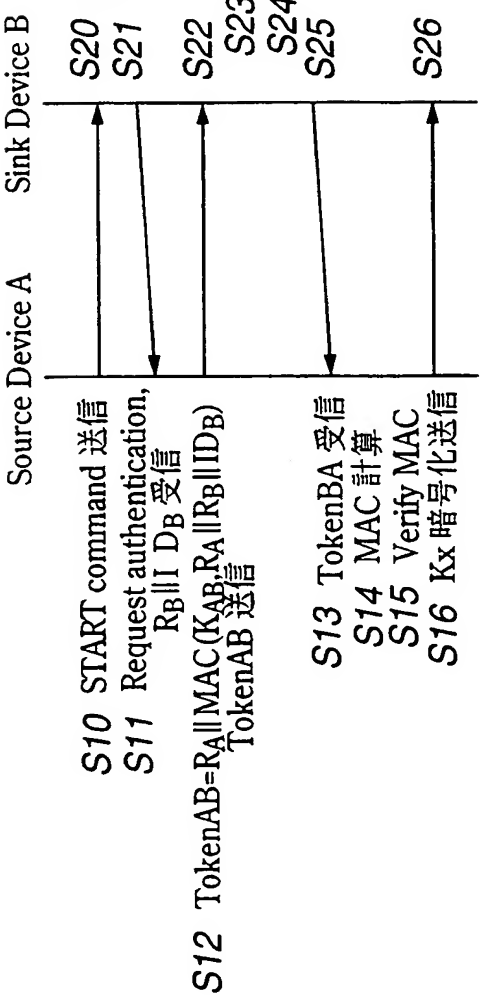


FIG.4

BNSDOCID: <WO___0062476A1_I_>

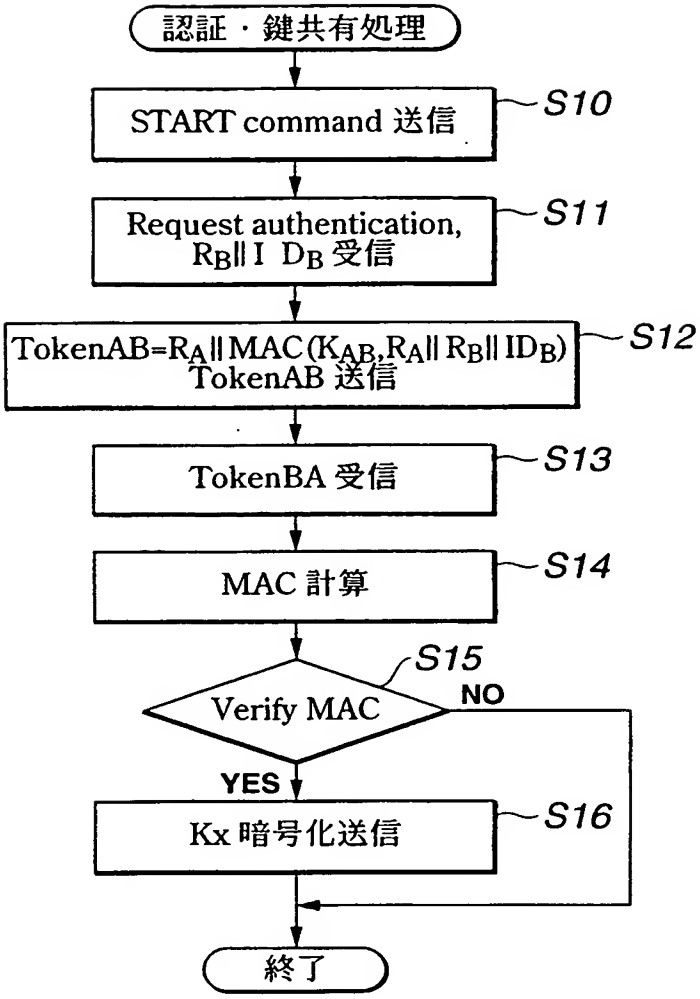

認証・鍵共有処理
START command 送信
S10
Request authentication, RB‖I DB 受信
S11
TokenAB=RA‖MAC(KAB,RA‖RB‖IDB) TokenAB 送信
S12
TokenBA 受信
S13
MAC 計算
S14
Verify MAC
S15
NO
YES
Kx 暗号化送信
S16
終了

FIG.5

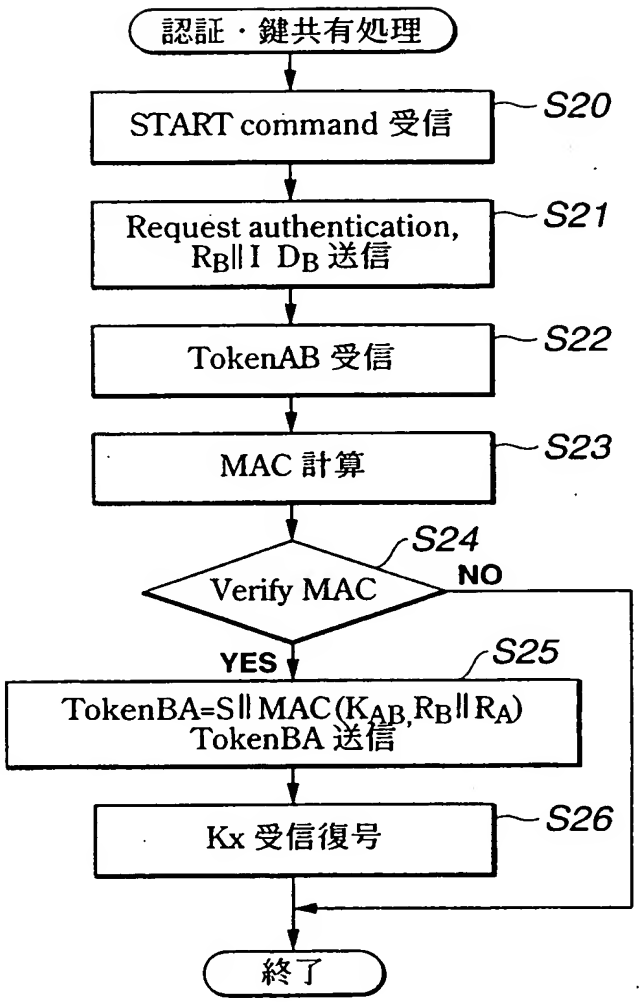

認証・鍵共有処理
START command 受信
S20
Request authentication,
RB‖I DB 送信
S21
TokenAB 受信
S22
MAC 計算
S23
S24
Verify MAC
NO
YES
S25
TokenBA=S‖MAC(KAB,RB‖RA)
TokenBA 送信
Kx 受信復号
S26
終了

FIG.6

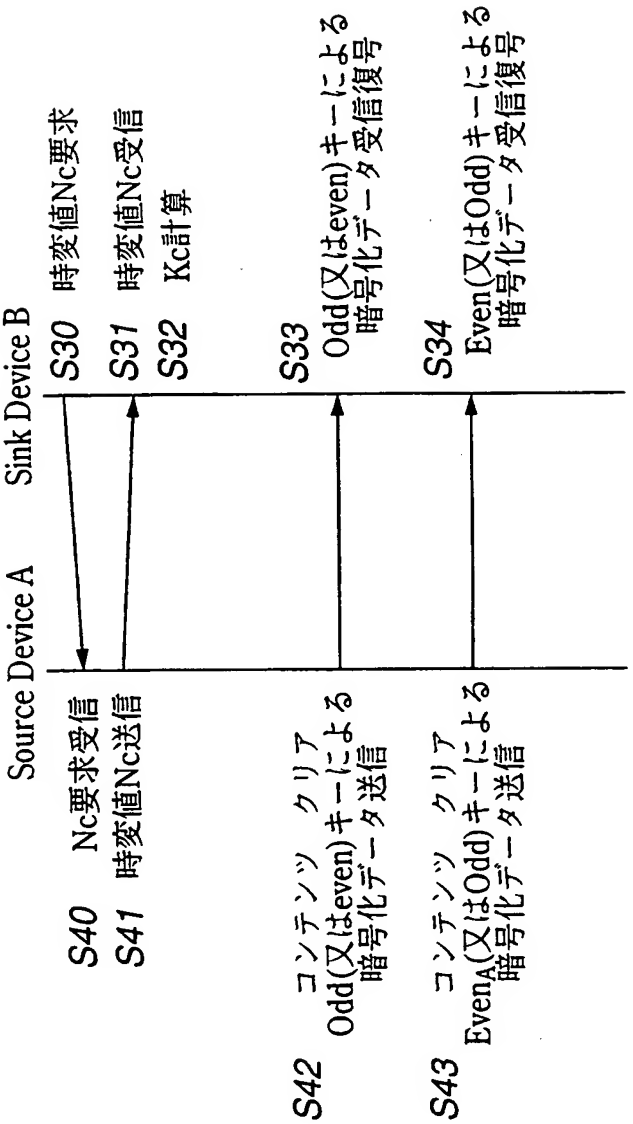


FIG.7

UNSUCCID:<WO 0062476A1_I_>

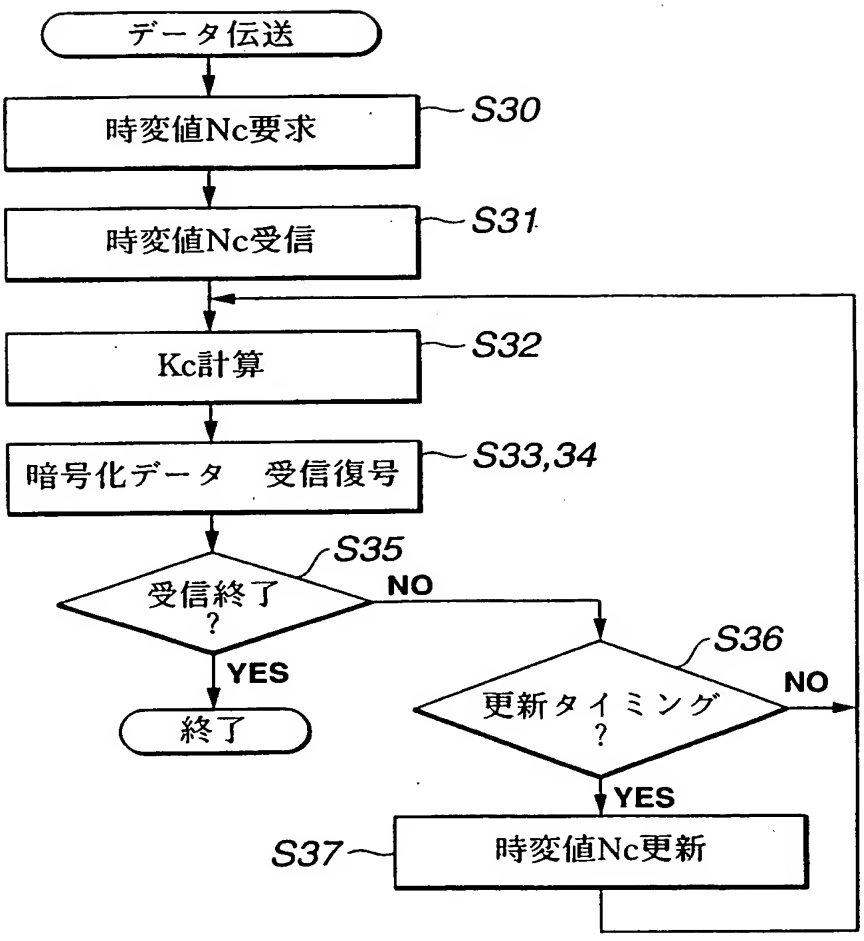

データ伝送
時変値Nc要求
S30
時変値Nc受信
S31
Kc計算
S32
暗号化データ　受信復号
S33,34
S35
受信終了
?
NO
YES
終了
S36
更新タイミング
?
NO
YES
S37
時変値Nc更新

FIG.8

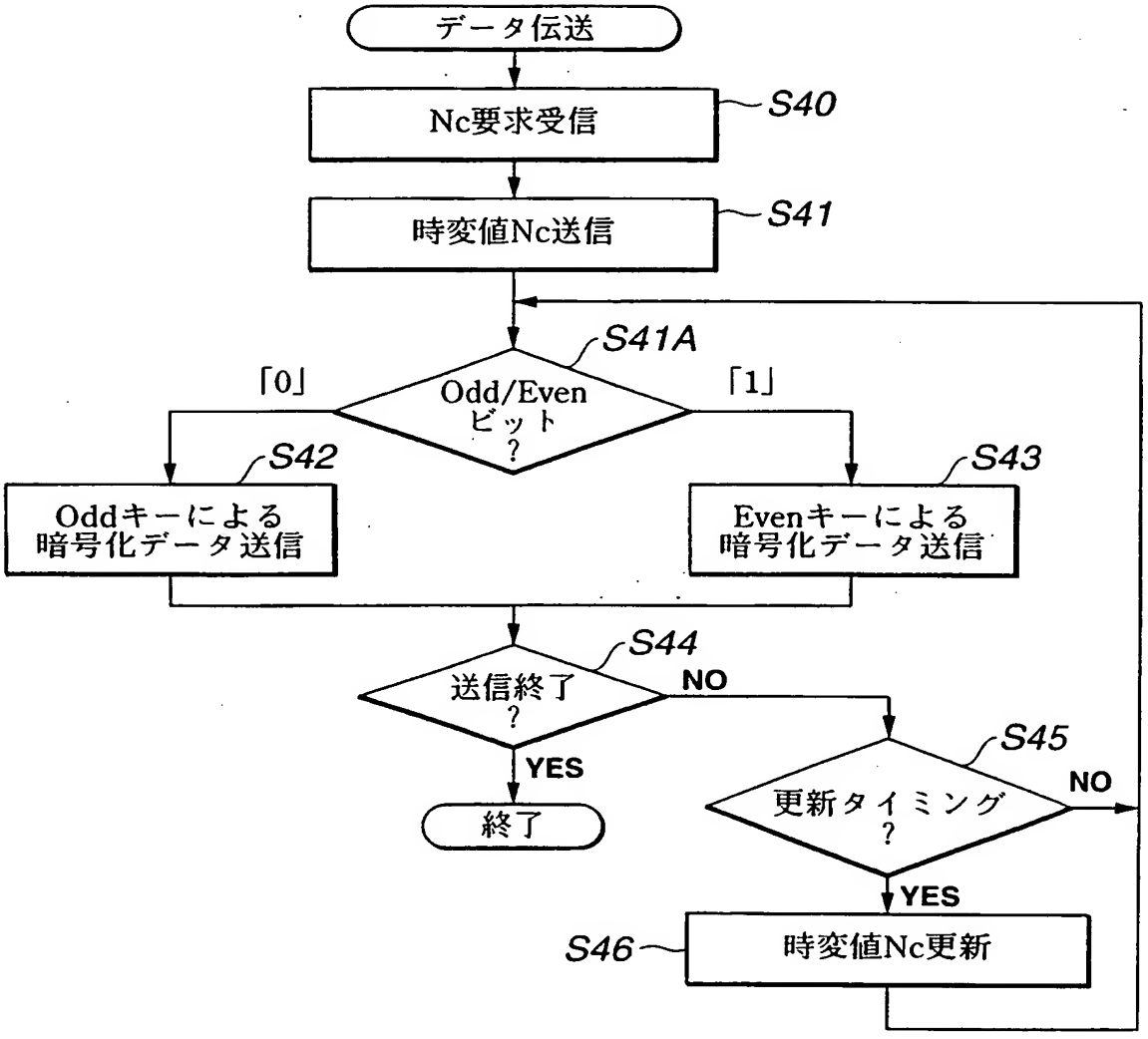


FIG.9

BNSDOCID: <WO___0062476A1_I_>

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP00/02354

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] H04L9/08, H04L9/32, H04L12/40, H04N7/167

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] H04L9/08, H04L9/32, H04L12/40, H04N7/167

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1926-1996 Toroku Jitsuyo Shinan Koho 1994-2000
Kokai Jitsuyo Shinan Koho 1971-2000 Jitsuyo Shinan Toroku Koho 1996-2000

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	Ryuji Ishiguro "Angou Gijutsu wo Tsukatta IEEE1394 jo no Computer Protection", Proceedings of Sony Research Forum 1997, Vol.7th (01.02.98) p.203-208	1-44
Y	Hitachi, Ltd. et al., "5C Digital Transmission Content Protection White Paper", Revision 1.0 http://www.dtcp.com/wp_spec.pdf (14.07.98)	1-44
Y	JP, 4-277951, A (NEC Corporation), 02 October, 1992 (02.10.92), page 1, Column 1, lines 1 to 30; Figs. 1 to 7 & EP, 502441, A & CA, 2062170, A & US, 5251258, A & DE, 69227936, A	1,8,9,14, 21,26,31,38
Y	JP, 1-165241, A (Mitsubishi Electric Corporation), 29 June, 1989 (29.06.89), page 2, lower right column, lines 1 to 13; Figs. 1 to 2 (Family: none)	1,9,14,21, 26,31,38
Y	JP, 10-4403, A (NTT Data Tsushin K.K.), 06 January, 1998 (06.01.98),	4,12,17,24, 29,34,41

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
04 July, 2000 (04.07.00)	18 July, 2000 (18.07.00)
Name and mailing address of the ISA/ Japanese Patent Office	Authorized officer
Facsimile No.	Telephone No.

Form PCT/ISA/210 (second sheet) (July 1992)

BNSDOCID: <WO___0062476A1_I_>

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP00/02354

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
	page 5, Column 7, line 10 to page 6, Column 9, line 2; Figs. 1 to 4 (Family: none)	
A	Teruyoshi Komuro "Av wo Multi Media ka Suru IEEE1394 no Genjo to Tenbo" Denshi Gijutsu March, Vol.41, No.3 (01.03.99) pp.2-7	1-44
A	JP, 10-303945, A (Sony Corporation), 13 November, 1998 (13.11.98), Full text; Figs. 1 to 6 & KR, 98081633, A	1-44

BNSDOCID: <WO 0062476A1 | >

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ００／０２３５４

A.　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Ｉｎｔ．Ｃｌ⁷　　Ｈ０４Ｌ９／０８，Ｈ０４Ｌ９／３２，Ｈ０４Ｌ１２／４０，Ｈ０４Ｎ７／１６７

B.　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Ｉｎｔ．Ｃｌ⁷　　Ｈ０４Ｌ９／０８，Ｈ０４Ｌ９／３２，Ｈ０４Ｌ１２／４０，Ｈ０４Ｎ７／１６７

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２６－１９９６年
日本国公開実用新案公報	１９７１－２０００年
日本国登録実用新案公報	１９９４－２０００年
日本国実用新案登録公報	１９９６－２０００年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Ｙ	石黒隆二：“暗号技術を使ったＩＥＥＥ１３９４上のコンピュータプロテクション” Proceedings of Sony Research Forum 1997（ソニーリサーチフォーラム１９９７論文集）， Ｖｏｌ．７ｔｈ　（０１．０２．９８）　ｐ．２０３－２０８	１－４４
Ｙ	Hitachi,Ltd.他：“5C Digital Transmission Content Protection White Paper”,Revision1.0 http://www.dtcp.com/wp_spec.pdf（１４．０７．９８）	１－４４

☒ Ｃ欄の続きにも文献が列挙されている。　　☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの
「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「Ｏ」口頭による開示、使用、展示等に言及する文献
「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「＆」同一パテントファミリー文献

国際調査を完了した日 ０４．０７．００	国際調査報告の発送日　**18.07.00**
国際調査機関の名称及びあて先 日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	特許庁審査官（権限のある職員） 青木　重徳　印　5W　4229 電話番号　０３－３５８１－１１０１　内線　３５７４

様式ＰＣＴ／ＩＳＡ／２１０（第２ページ）（１９９８年７月）

BNSDOCID: <WO___0052476A1_I_>

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ００／０２３５４

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Ｙ	ＪＰ，４－２７７９５１，Ａ　（日本電気株式会社） ２．１０月．１９９２　（０２．１０．９２） 第１頁第１欄第１－３０行，図１－７ ＆ ＥＰ，５０２４４１，Ａ ＆ ＣＡ，２０６２１７０，Ａ ＆ ＵＳ，５２５１２５８，Ａ ＆ ＤＥ，６９２２７９３６，Ａ	1, 8, 9, 14, 21, 26, 31, 38
Ｙ	ＪＰ，１－１６５２４１，Ａ （三菱電機株式会社） ２９．６月．１９８９　（２９．０６．８９） 第２頁右下欄第１－１３行，第１－２図 （ファミリーなし）	1, 9, 14, 21, 26, 31, 38
Ｙ	ＪＰ，１０－４４０３，Ａ （エヌ・ティ・ティ・データ通信株式会社） ６．１月．１９９８　（０６．０１．９８） 第５頁第７欄第１０行－第６頁第９欄第２行，図１－４ （ファミリーなし）	4, 12, 17, 24, 29, 34, 41
Ａ	小室輝芳；“ＡＶをマルチメディア化するＩＥＥＥ１３９４の現状と展望” 電子技術　３月号，Ｖｏｌ．４１，Ｎｏ．３ （０１．０３．９９）　ｐ．２－７	１－４４
Ａ	ＪＰ，１０－３０３９４５，Ａ （ソニー株式会社） １３．１１月．１９９８　（１３．１１．９８） 全文，図１－６ ＆ ＫＲ，９８０８１６３３，Ａ	１－４４

様式ＰＣＴ／ＩＳＡ／２１０（第２ページの続き）（１９９８年７月）

BNSDOCID: <WO 0062476A1 I >